RSAC 2025 Conference

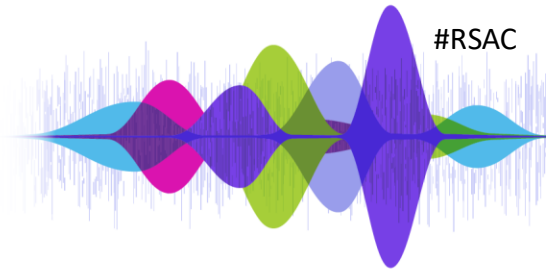
Many Voices.
One Community.

SESSION ID: CLS-W01

GCP Organization Policies to Live By - And Their Implementation Pitfalls

Kat Traxler

Principal Security Researcher – Public Cloud
Vectra AI
https://kat.omg.lol



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

About me

Kat Traxler

Security Research

- Vectra AI Principal Security Researcher
- IANS Faculty

*"Excited about exploring where technology **boundaries intersect** and are stitched together with protocols and assumptions"*

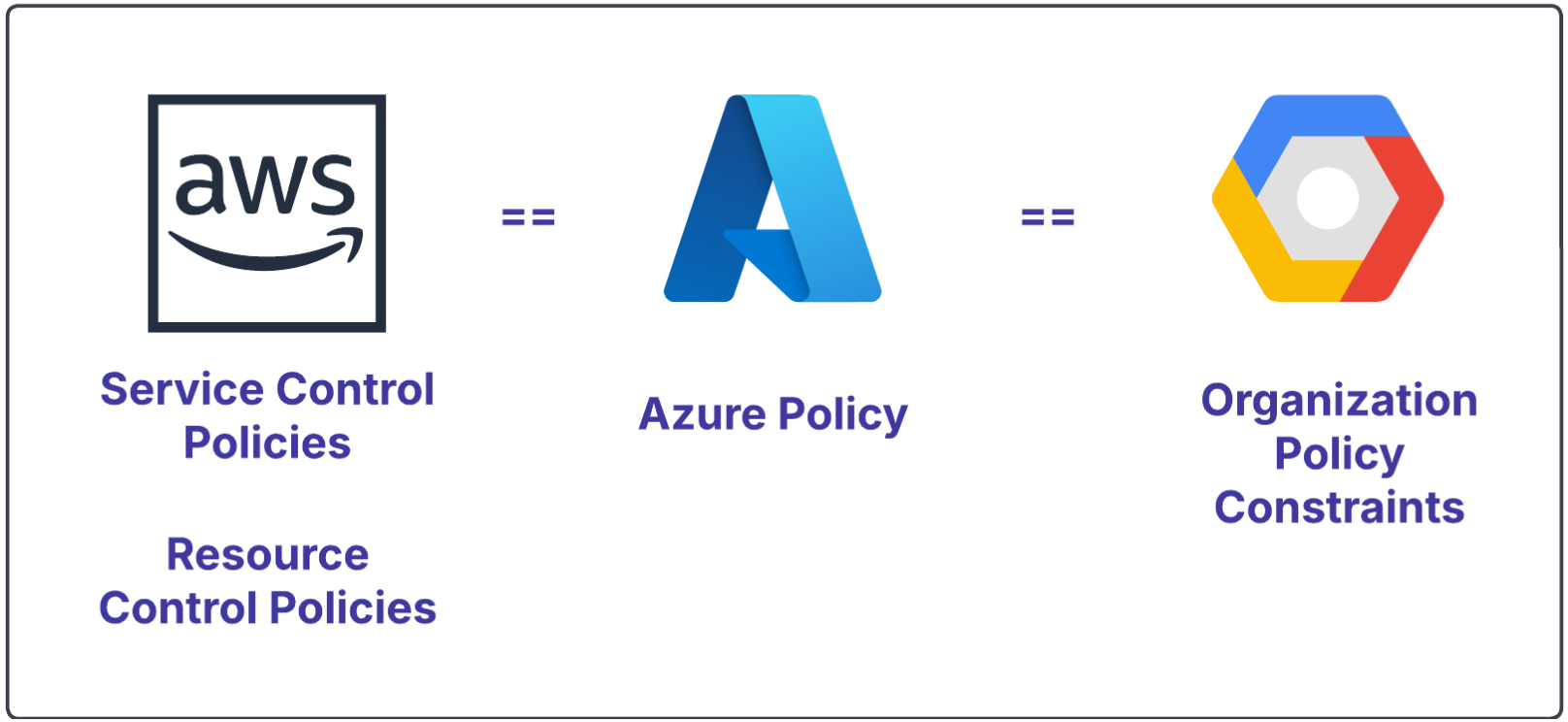
Agenda

- Mega Corp Moves to the Cloud
- Org Policy Constraints to Live By
  - Org Policies | 101
  - Great Guardrails for Risk Reduction
- When Cloud Gets Real
  - Implementation Challenges
- We Secure the Cloud We Have; Not the One We Want
  - Adapting Enforcement to Reality

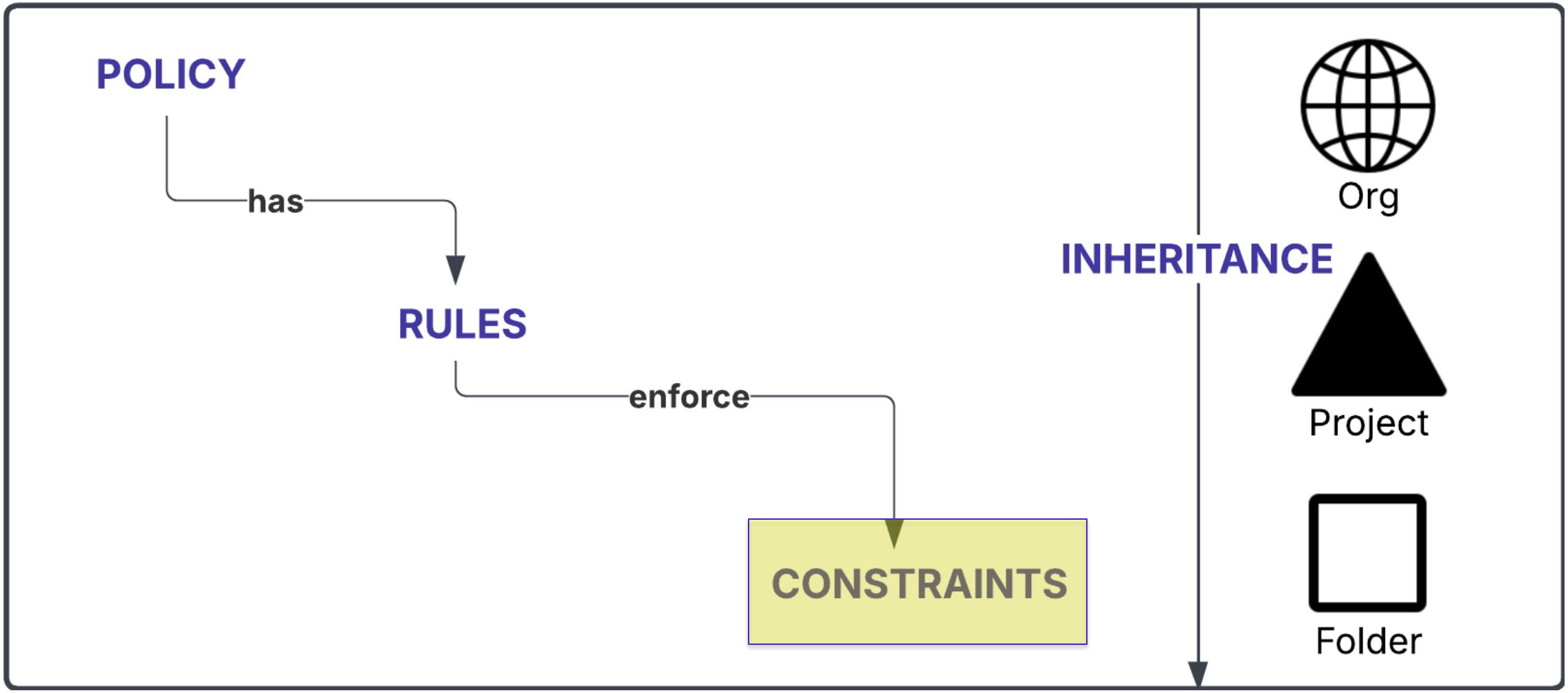
Mega Corp Moves to the Cloud

Guardrails for your Cloud

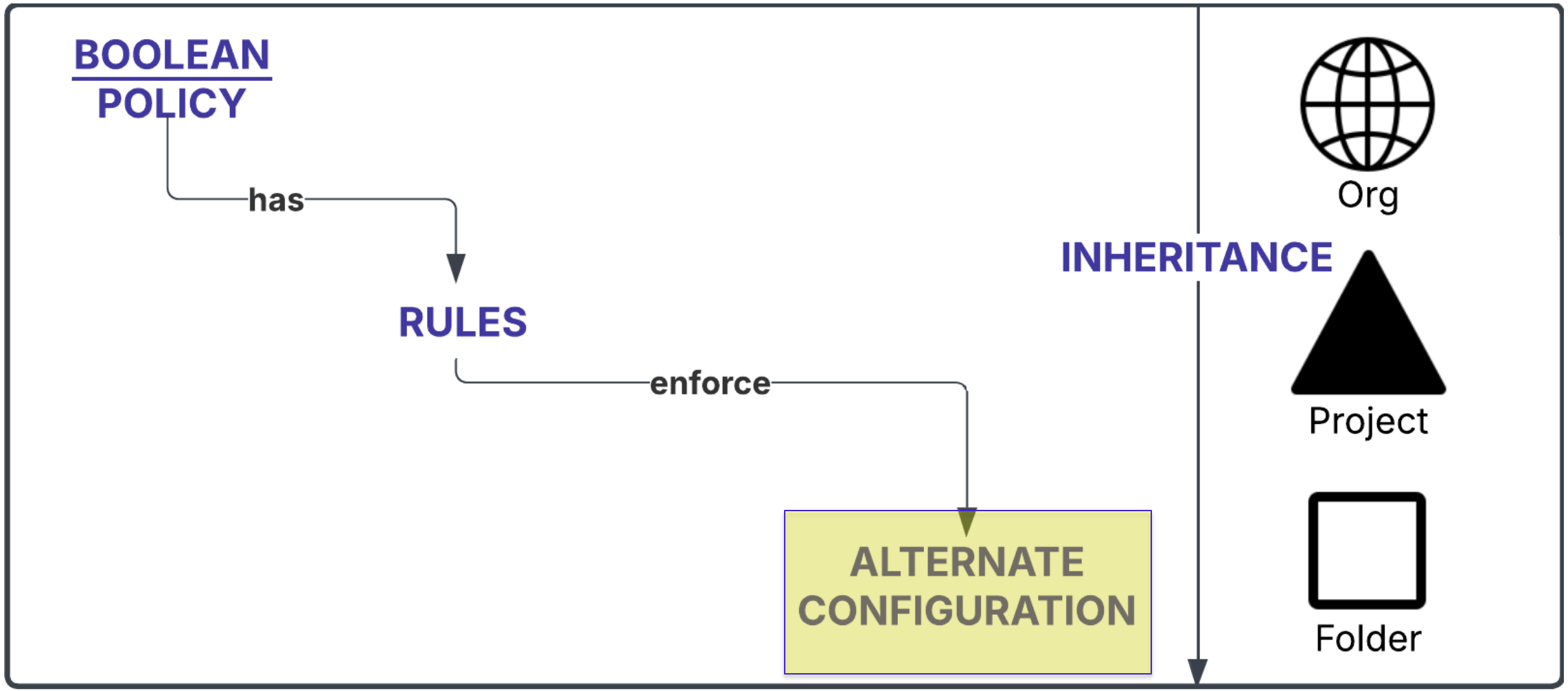
- A GCP Organization Policy is a set of **rules and constraints** that govern how resources in your Google Cloud environment can be used.



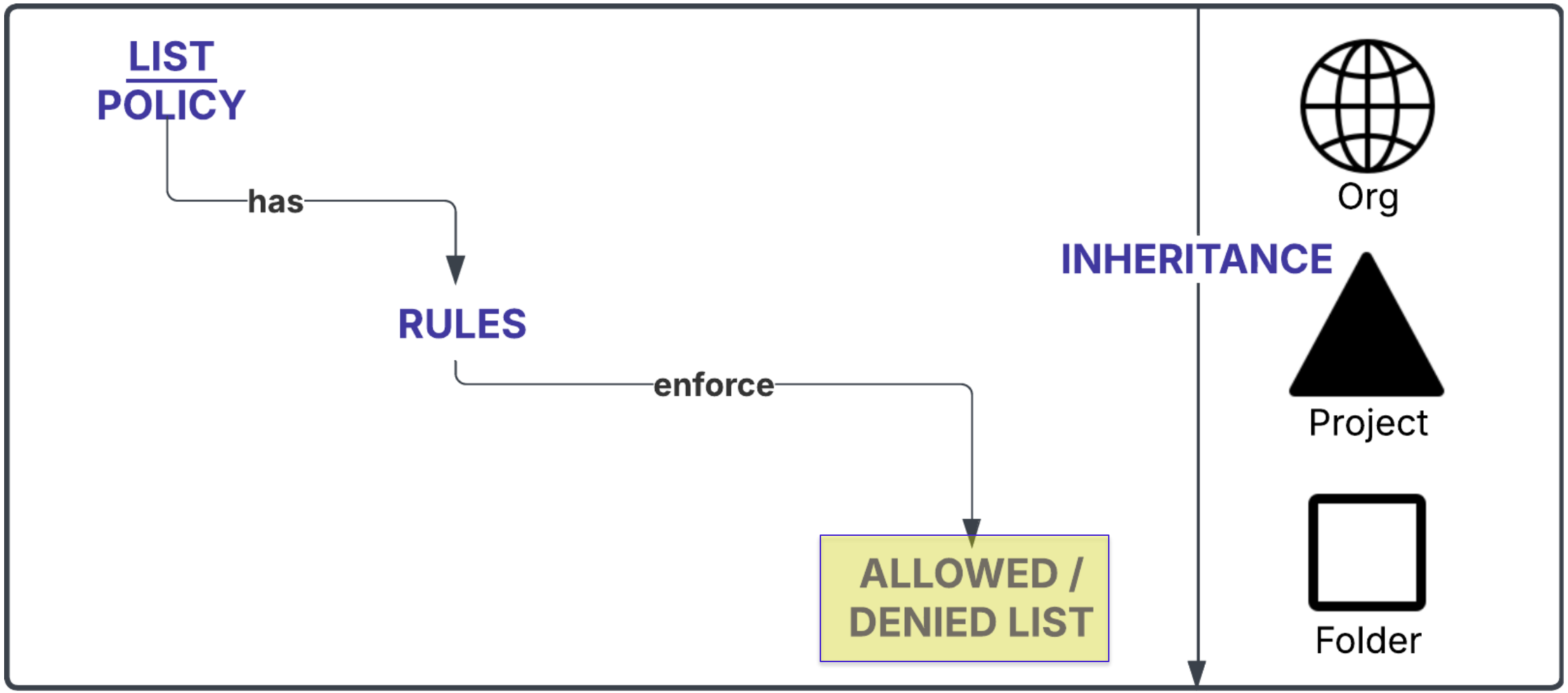
Organization Policy Concepts



Organization Policy Concepts – Boolean Constraints



Organization Policy Concepts – List Constraints



RSAC 2025 Conference

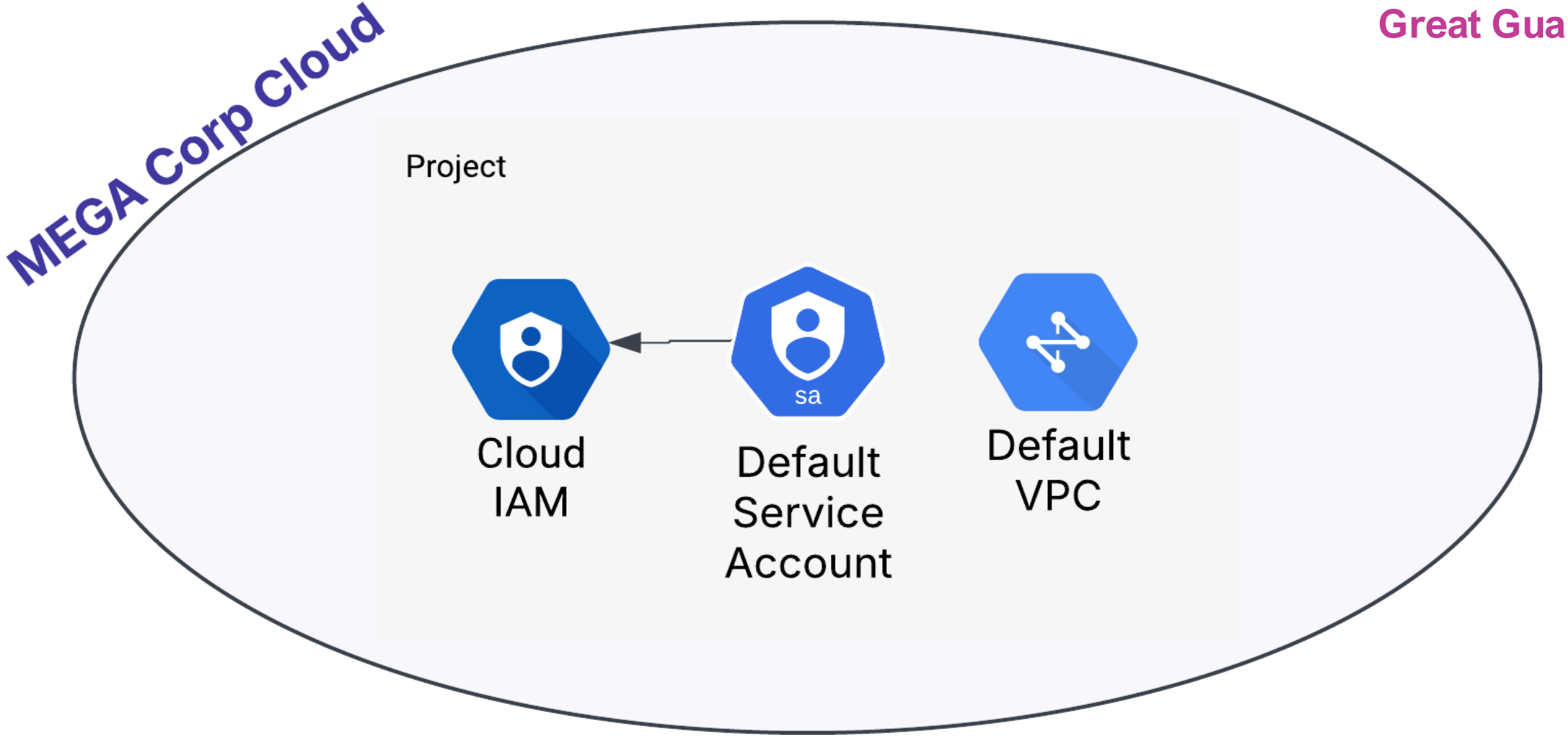
Great Guardrails

Policies to Shape Your Exposure to Risk

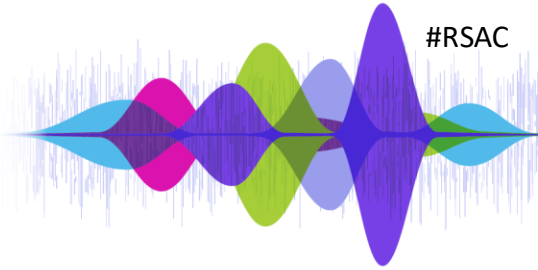
Many Voices.
One Community.

Disable Risky Defaults

Great Guardrails



Enforce a More Mature Cloud

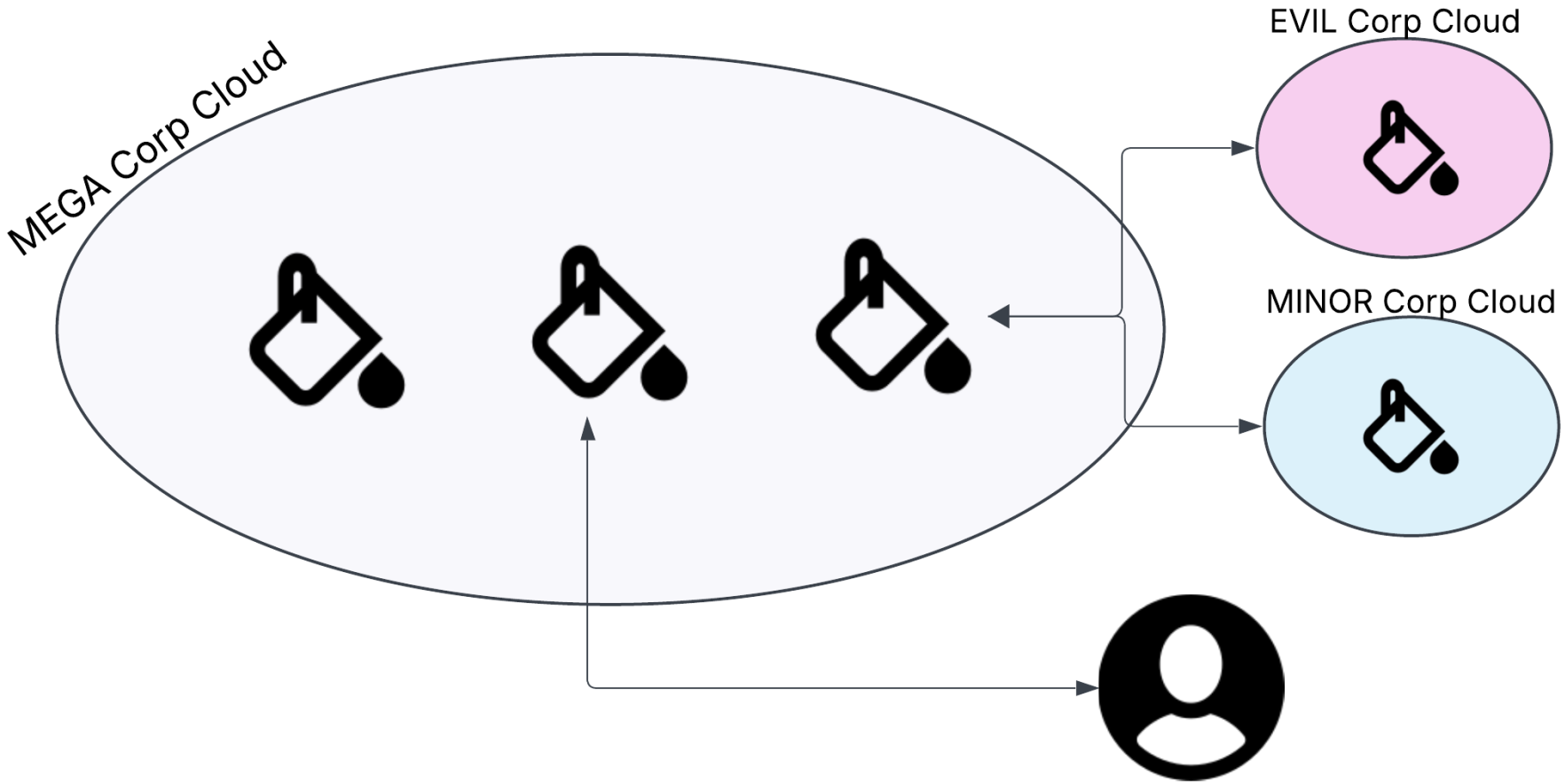


Great Guardrails

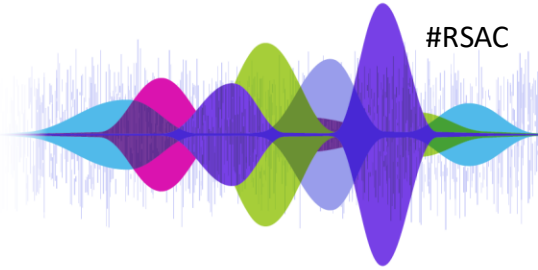
- Default Service Accounts
  - Disable Automatic IAM Grants for Default Service Accounts
    - `constraints/iam.automaticIamGrantsForDefaultServiceAccounts`
  - Disable Create Default Service Account (Cloud Build)
    - `constraints/cloudbuild.disableCreateDefaultServiceAccount`
- Skip default network creation
  - constraints/compute.skipDefaultNetworkCreation

Tackle Data Exfiltration Risks in PaaS

Great Guardrails



Define an Identity Perimeter with Org Policies

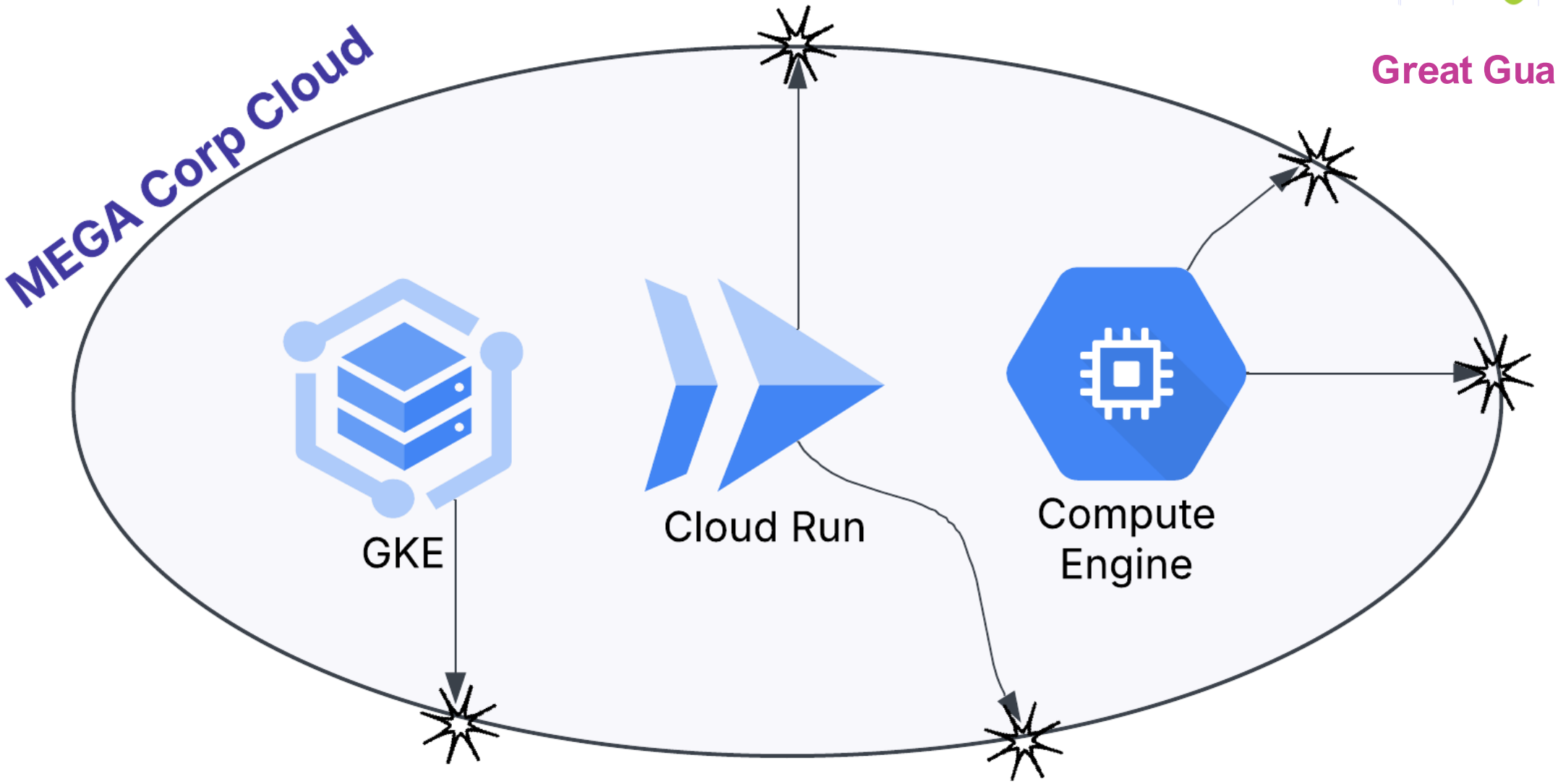


Great Guardrails

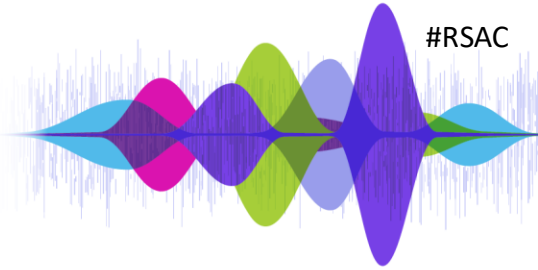
- Allowed external Identity Providers for workloads in Cloud IAM
  - `constraints/iam.workloadIdentityPoolProviders`
- Allowed AWS accounts that can be configured for workload identity federation in Cloud IAM
  - `constraints/iam.workloadIdentityPoolAwsAccounts`
- Domain restricted sharing
  - `constraints/iam.allowedPolicyMemberDomains`
- Cloud Storage - restrict authentication types
  - `constraints/storage.restrictAuthTypes`

Limit Exposed Endpoints

Great Guardrails



Restrict your Network Perimeter with Org Policies

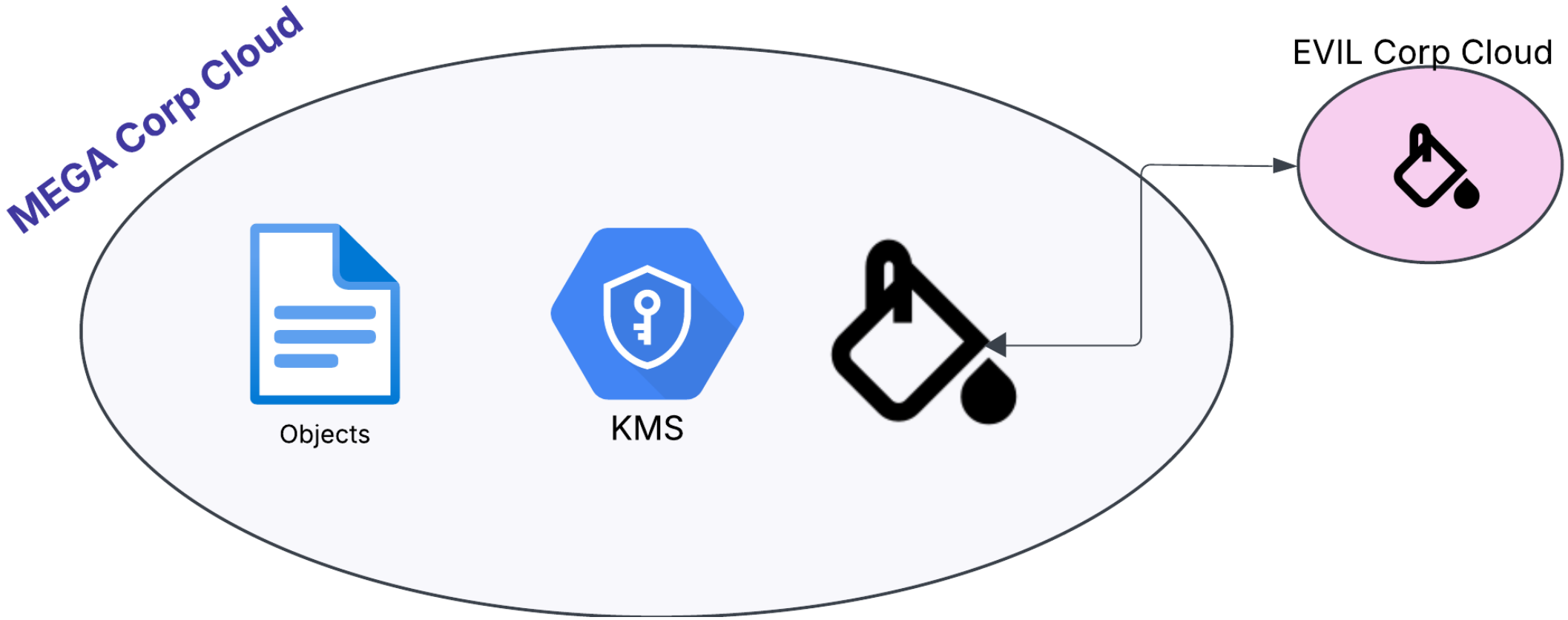


Great Guardrails

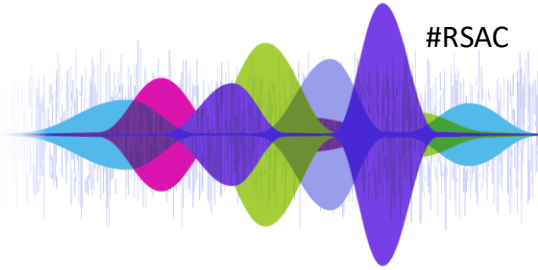
- Define allowed external IPs for VM instances
  - `constraints/compute.vmExternalIpAccess`
- Restrict Public IP access on Cloud SQL instance
  - `constraints/sql.restrictPublicIp`
- Allowed ingress settings (Cloud Run)
  - `constraints/run.allowedIngress`
- Skip default network creation
  - constraints/compute.skipDefaultNetworkCreation

Ransomware - Preventing the 2am Call

Great Guardrails



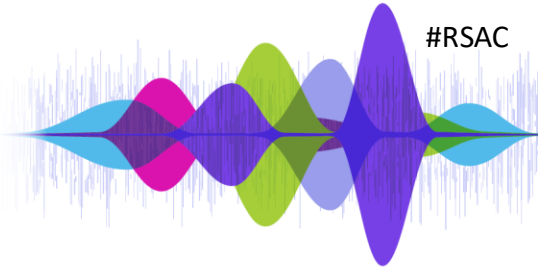
Data-centric Security with Org Policy



Great Guardrails

- Storage Bucket Constraints
  - Enforce Public Access Prevention
    - `constraints/storage.publicAccessPrevention`
  - Enforce uniform bucket-level access
    - `constraints/storage.uniformBucketLevelAccess`
- KMS Key Constraints
  - Minimum destroy scheduled duration per key
    - `constraints/cloudkms.minimumDestroyScheduledDuration`
  - Restrict which projects may supply KMS CryptoKeys for CMEK
    - `constraints/gcp.restrictCmekCryptoKeyProjects`

Classes of Vulnerabilities Prevented



- Over-permissioned Default Service Accounts
- Publicly Exposed Resources
- Unauthorized Access Outside of MegaCorp Domain
- Open Management Ports
- Cloud-Native Ransomware Tactics

RSAC | 2025 Conference

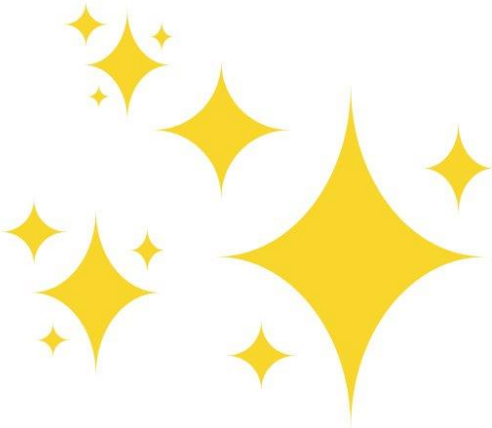
Implementation Challenges

When Cloud Gets Real

Many Voices.
One Community.

Mega Corp Builds the Perfect Greenfield Cloud

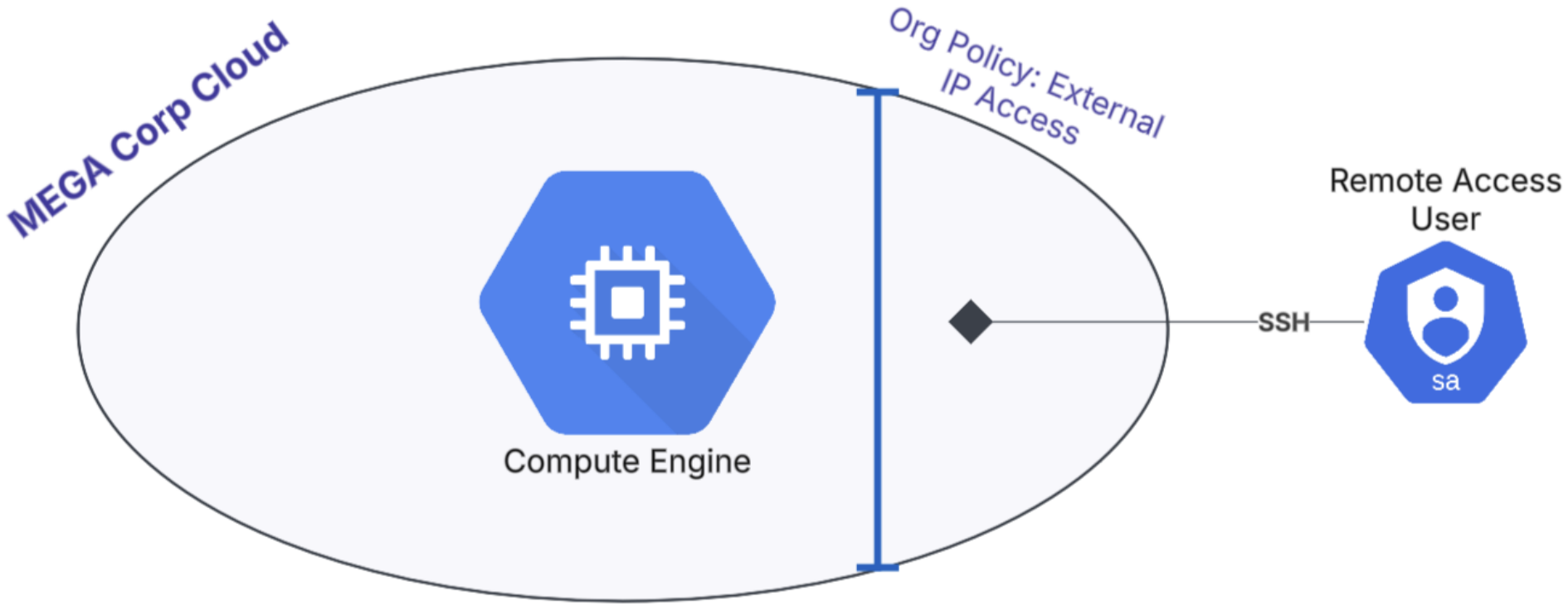
A perfectly hardened cloud environment has been molded using **Organization Policies**, constraining the environment, effectively banning the riskiest configurations and behavior.



Failing to Provide Alternatives to Defaults – Remote Access

Implementation Challenges

- Compute VM that are allowed to use external IP addresses
  - `constraints/compute.vmExternalIpAccess`



Failing to Provide Alternatives to Defaults – Resource Identity

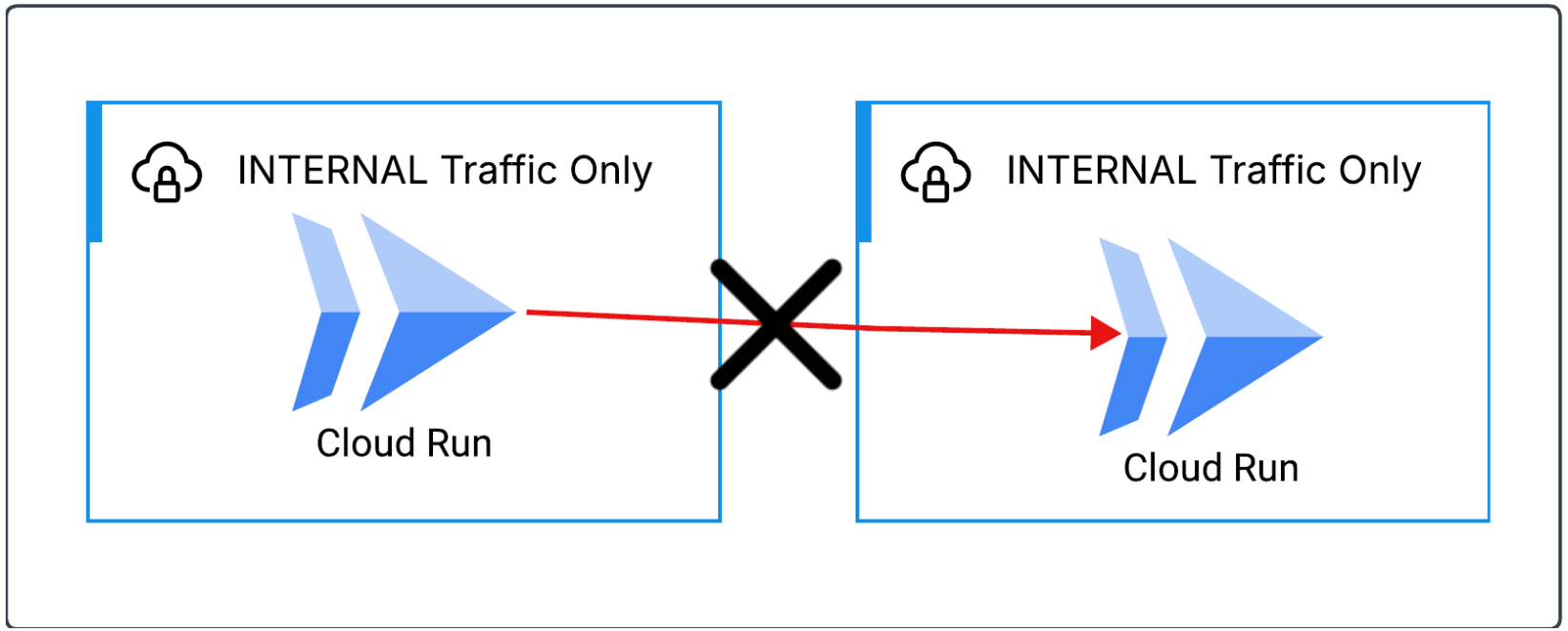
Implementation Challenges

- Disable Automatic IAM Grants for Default Service Accounts
  - `constraints/iam.automaticIamGrantsForDefaultServiceAccounts`
- Disable Create Default Service Account (Cloud Build)
  - `constraints/cloudbuild.disableCreateDefaultServiceAccount`

Unintended Consequences – Breaking Patterns

Implementation Challenges

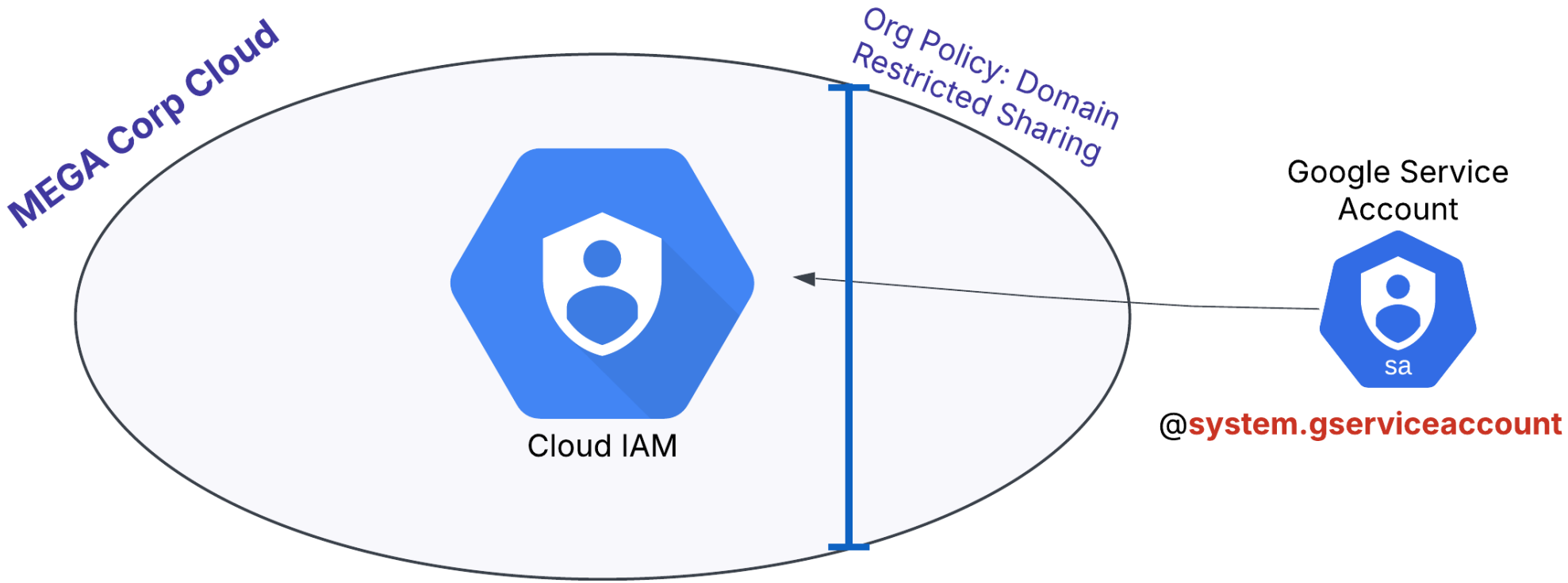
- Allowed ingress settings (Cloud Run)
  - `constraints/run.allowedIngress`



Unintended Consequences – Wait, I Can't Integrate with Google?

Implementation Challenges

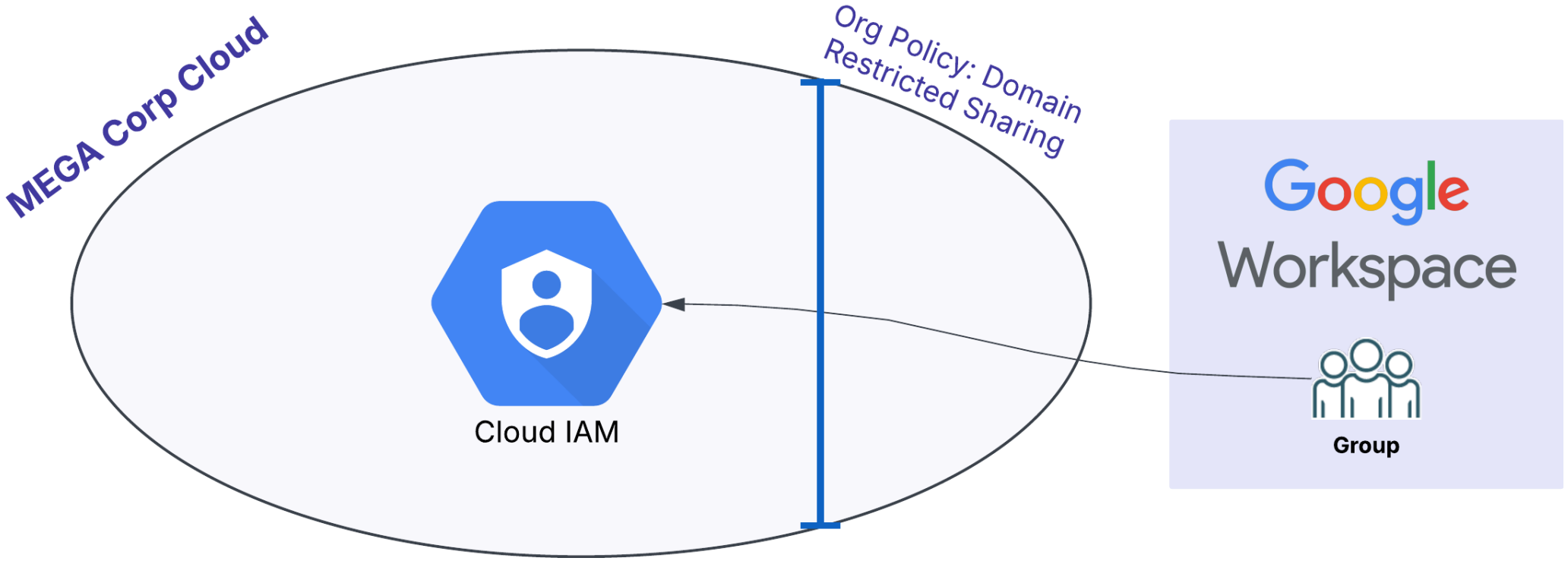
- Domain restricted sharing
  - `constraints/iam.allowedPolicyMemberDomains`



Organization Policy Bypasses

Implementation Challenges

- Domain restricted sharing
  - `constraints/iam.allowedPolicyMemberDomains`



RSAC 2025 Conference

We Secure the Cloud We Have

Not The One We Want

Mega Corp Adapts To Their Cloudy Reality

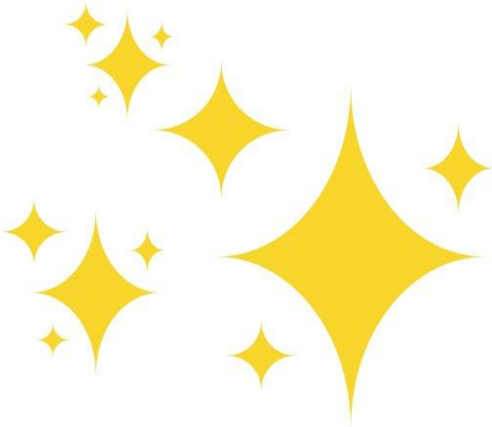
Exception requests are drowning Security Teams and slowing the speed of cloud adoption. How will Mega Corp **manage these invariants**?

Adapting Organization Policy Enforcement

- **The ‘Toggle Method’**
  - Organization Policies are not retroactive – toggling a policy on/off can be used for exceptions
  - Results in a loosely documented non-compliant configuration
- **Architect Dual Enforcement Zones**
  - Apply policies at the folder-level, leverage inheritance to define separate policy zones
  - Organic growth is inevitable, coloring in the lines is hard.

Preventative Controls Match Cloud Maturity

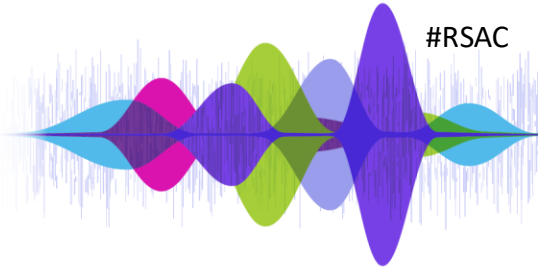
Organization Policy **enforcement is aligned with cloud maturity**. As Mega Corp disseminates known-good patterns, only then can they move beyond defaults and operate in a more secure configuration



Organization Policy Enforcement in your OKRs

- **Objective:** Strengthen Google Cloud security configuration and ensure compliance with industry best practices.
  - **Key Result 1:** Achieve 100% enforcement of the "Restrict Public IP Addresses" Organization Policy across all projects within the production folder by the end of Q3.
  - **Key Result 2:** Reduce the number of exceptions to the "Default Cloud Build Service Account" Organization Policy by 50% within the development folder.
  - **Key Result 3:** Implement and enforce the "Enforce uniform bucket-level access" Organization Policy for all Buckets in the PCI-DSS compliant folder.
  - **Key Result 4:** Automate the detection and remediation of violations against the "Domain Restricted Sharing" Organization policy, with a maximum remediation time of 5 day.

Apply Org Policies with Eyes Wide Open



- Next week you should:
  - Know which Org Policies are **currently enforced** in your GCP environment
  - Understand the safety guardrails Org Policies can bring to your cloud
- In the first three months following this presentation you should:
  - Identify Org Policies as goals and **codify as KPI's**
  - Alert business to possible pitfalls and challenges when enforcing Org Policies
  - **Develop a plan** for maturing cloud to allow for smoother Org Policy implementation
- Within six months you should:
  - Achieved the **enablement of a key Org Policy** with minimal business disruption

RSAC™ 2025 Conference

Many Voices.
One Community.

For more information:

www.vectra.ai/about/author/kat-traxler